https://doi.org/10.31891/2307-5732-2025-359-105
УДК 004.79:629.85

НІКОНОВ ОЛЕГ
Київський національний університет технологій та дизайну
https://orcid.org/0000-0002-8878-4318
e-mail: nikonov.oy@knutd.edu.ua
ФІЛІПОВ ВЯЧЕСЛАВ
Київський національний університет технологій та дизайну
https://orcid.org/0000-0001-7854-6693
e-mail: mv650434@gmail.com

СИСТЕМА МОНІТОРИНГУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОГО КОМПЛЕКСУ НАЗЕМНИХ МОБІЛЬНИХ РОБОТИЗОВАНИХ ПЛАТФОРМ

Представлено концепцію побудови системи моніторингу інформаційно-комунікаційного комплексу наземних мобільних роботизованих платформ, спрямовану на забезпечення надійності, безперервності та захищеності функціонування ключових інформаційних підсистем. Обґрунтовано необхідність комплексного контролю стану сенсорних модулів, каналів зв'язку, обчислювальних блоків і виконавчих елементів у реальному часі. Запропоновано архітектуру системи моніторингу, що базується на використанні телеметрії, діагностичних алгоритмів, методів визначення критичних параметрів та механізмів забезпечення інформаційної безпеки. Проведено аналіз сучасних підходів та визначено перспективи впровадження систем моніторингу наземних мобільних роботизованих платформ з метою підвищення їх автономності, живучості та стійкості до загроз екзогенного характеру.

Ключові слова: *моніторинг, інформаційно-комунікаційний комплекс, роботизовані платформи, телеметрія, діагностика, інформаційна безпека*

NIKONOV OLEH, FILIPOV VIACHESLAV
Kyiv National University of Technology and Design

MONITORING SYSTEM OF THE INFORMATION AND COMMUNICATION COMPLEX OF GROUND MOBILE ROBOTIC PLATFORMS

The article presents an advanced concept of a monitoring system designed for the information and communication complex of ground mobile robotic platforms. The proposed approach is aimed at ensuring stable, secure and high-performance functioning of robotic systems that operate in dynamic, uncertain and technologically challenging environments. Ground mobile robotic platforms rely on a coordinated interaction between sensor modules, communication channels, computing units and executive components, all of which must maintain reliable operation to guarantee autonomous navigation, perception of the surrounding space and correct execution of assigned missions. In practical applications these elements are influenced by mechanical impacts, unpredictable environmental changes, electromagnetic disturbances, cyberattacks and internal failures, which significantly increases the need for an integrated monitoring and diagnostic infrastructure.

The monitoring system proposed in the article unifies multi-source telemetry processing, real-time diagnostic procedures, detection of abnormal behaviour, prediction of potential failures and information security mechanisms within a single architectural framework. Special emphasis is placed on identifying critical parameters that describe the operational state of sensor systems, wireless and wired communication channels, on-board computational modules and motion control subsystems. The system incorporates intelligent diagnostic algorithms based on statistical methods, machine learning techniques and models of fuzzy logic. These methods enable early detection of hidden malfunctions, gradual degradation of components and deviations that may lead to mission failure. Furthermore, the monitoring architecture includes information protection mechanisms that ensure resistance to signal substitution, intentional distortion of navigation data, blocking of communication channels, unauthorized access attempts and other forms of external interference.

The practical significance of the proposed solution is manifested in its ability to increase the autonomy, survivability and operational stability of ground mobile robotic platforms in complex or high-risk conditions. The monitoring system can be integrated into existing robotic platforms without a need for substantial modifications of their structure. It enables continuous assessment of the technical condition of key components, automatic transition to backup communication or control modes, protection of internal and external information flows and timely notification of the operator about emerging threats or failures.

Keywords: *monitoring, information and communication complex, robotic platforms, telemetry, diagnostics, information security*

Стаття надійшла до редакції / Received 22.10.2025
Прийнята до друку / Accepted 15.11.2025

Постановка проблеми

Новітні наземні мобільні роботизовані платформи (НМРП) активно інтегруються у оборонну сферу, логістику, промисловість та системи цивільного захисту. НМРП виконують широкий спектр функцій: від розвідки та моніторингу середовища до транспортування вантажів, підтримки підрозділів, розмінування територій і виконання спеціальних тактичних завдань. Ефективність їх роботи безпосередньо залежить від надійності інформаційно-комунікаційного комплексу (ІКК), який забезпечує збір даних, обмін інформацією, керування рухом, взаємодію з оператором та виконання автоматизованих функцій [1-4].

В умовах нестабільності та високої динаміки середовища, впливу електромагнітних перешкод, кібератак, механічних ушкоджень та відмов компонентів важливим стає оперативний контроль стану всіх підсистем. Недостатня увага до процесів моніторингу призводить до зниження автономності, втрати керованості, появи аномальних дій платформи та збільшення ризику втрати її працездатності.

Тому однією з ключових задач сучасної робототехніки є створення системи моніторингу ІКК, здатної: контролювати працездатність сенсорів, каналів зв'язку, обчислювальних модулів; виявляти ранні ознаки відмов; прогнозувати критичні стани; забезпечувати захищеність інформації; підтримувати адаптивну реакцію

НМРП у реальному часі.

Проблема полягає у відсутності комплексних рішень, які б інтегрували механізми моніторингу на всіх рівнях функціонування НМРП та забезпечували глибоку діагностику ІКК з метою підвищення автономності, живучості та стійкості НМРП до загроз екзогенного характеру.

Аналіз останніх досліджень і публікацій

Проблематика моніторингу роботизованих систем упродовж останніх років набула особливого значення у зв'язку зі зростанням складності та їх залежності від інформаційно-комунікаційної інфраструктури. Огляд останніх досліджень і публікацій свідчить, що інтенсивний розвиток відбувається водночас у кількох ключових напрямах, які охоплюють машинне навчання для технічної діагностики, мультисенсорні системи, дослідження стійкості до зовнішніх впливів та методи забезпечення кібербезпеки [5-8].

У напрямку технічної діагностики роботи зосереджуються на застосуванні моделей машинного навчання для виявлення аномальних станів, прогнозування відмов і аналізу деградації компонентів. Підхід, заснований на інтелектуальній обробці телеметрії, дозволяє формувати прогноз технічного стану платформи, що значно підвищує її надійність та автономність у складних середовищах [1,5].

Другий напрям охоплює розвиток сенсорних систем, які забезпечують багатовимірне сприйняття середовища. Публікації останніх років зосереджені на вдосконаленні засобів мультисенсорної обробки даних від камер, лідарів, радарів та інерційних модулів, що дозволяє підвищити стабільність навігації та точність оцінювання динамічних змін середовища. Дослідження підтверджують, що ефективна інтеграція сенсорних потоків є не лише основою для навігаційних і керуючих алгоритмів, а й важливим елементом системи моніторингу стану платформи, оскільки дає змогу виявляти дефекти або відмову сенсорів за непрямими ознаками [2,6].

Значне місце у літературі займають роботи, присвячені дослідженню стійкості роботизованих систем до зовнішніх збурень. Дослідження моделюють поведінку НМРП у середовищах із перешкодами та агресивними зовнішніми факторами, що вимагає включення до системи моніторингу механізмів оцінювання доступності каналів зв'язку, рівня зовнішніх перешкод, якості сенсорного вимірювання та надійності дій виконавчих елементів. Пропонуються моделі, які дозволяють адаптувати роботу платформи в умовах обмеженої комунікації або часткової втрати окремих модулів [1,3,7].

Окремий напрям досліджень пов'язаний із забезпеченням інформаційної безпеки НМРП. У межах цього напряму досліджуються проблеми захисту внутрішніх і зовнішніх каналів передачі даних, запобігання навігаційним атакам, а також виявлення спроб підміни або блокування телеметрії. У сучасних робототехнічних системах загрози кіберпростору є причиною некоректної роботи або повної втрати керованості, тому безпека ІКК розглядається як необхідна складова загальної архітектури моніторингу [4,8].

Попри значні досягнення, аналіз публікацій виявляє і низку обмежень сучасних підходів. Головною проблемою є фрагментарність існуючих рішень: більшість робіт орієнтовані на дослідження лише окремих підсистем – сенсорних модулів, каналів зв'язку або засобів кіберзахисту. Натомість сучасні НМРП мають високу взаємозалежність між усіма підсистемами, тому відсутність єдиної моделі моніторингу створює ризики для стабільності їх роботи в реальних умовах.

Проведений аналіз свідчить про нагальну потребу створення цілісної системи моніторингу ІКК НМРП, яка має поєднувати оцінювання технічного стану апаратної частини, аналіз телеметричних потоків, контроль якості каналів зв'язку, діагностику сенсорних модулів, кіберзахист, а також здатність до прогнозування критичних станів. Саме інтегрований підхід дозволяє забезпечити цілісне розуміння оперативної обстановки, своєчасне виявлення загроз та підвищення надійності НМРП у складних умовах експлуатації.

Формулювання цілей статті

Метою статті є розроблення концепції системи моніторингу ІКК НМРП, що забезпечує: оцінку працездатності компонентів у реальному часі, виявлення відмов і аномальних станів, забезпечення захищеності інформаційного обміну, підвищення автономності та живучості НМРП.

Для досягнення мети необхідно вирішення задач:

1. Аналіз структури ІКК НМРП.
2. Визначення критичних параметрів, що потребують моніторингу.
3. Розробка архітектури системи моніторингу.
4. Обґрунтування механізмів забезпечення інформаційної безпеки.

Реалізація вищезазначених задач дозволить створити основу для впровадження інтегрованих систем моніторингу, здатних підвищити автономність, живучість та інформаційну безпеку НМРП.

Виклад основного матеріалу дослідження

ІКК НМРП є багаторівневою інтегрованою системою, що забезпечує взаємодію сенсорних модулів, обчислювальних ресурсів, виконавчих механізмів та телекомунікаційної інфраструктури. Архітектура ІКК визначає здатність платформи до автономного функціонування, стійкість до зовнішніх впливів та можливість виконання складних завдань. Аналіз сучасних підходів показує, що структура комплексу має включати взаємопов'язані апаратні, програмні та мережеві компоненти, які формують повний цикл від збору даних до прийняття рішень та передавання команд (рис. 1).

Основа ІКК – сенсорна підсистема, яка забезпечує безперервний збір параметрів навколишнього середовища та внутрішнього стану НМРП. До її складу входять засоби візуального спостереження, такі як камери різних спектральних діапазонів, а також вимірювальні пристрої, що забезпечують просторове

сканування та оцінювання відстаней. Інформація, отримана сенсорами, має різну природу, частоту оновлення та точність. Тому головним завданням є її синхронізація, попередня фільтрація та об'єднання у єдиній координатній системі. Сенсорні дані надходять до обчислювального ядра платформи, яке виконує функції аналізу інформаційних потоків, моделювання станів та генерування керуючих дій. Архітектура обчислювальної підсистеми передбачає наявність високопродуктивних процесорів, графічних прискорювачів та спеціалізованих модулів для обробки великих масивів даних у реальному часі. Критично важливим компонентом ІКК є телекомунікаційна підсистема, яка забезпечує зв'язок НМРП з операторськими центрами, іншими роботами та елементами інфраструктури. Передавання даних може здійснюватися за допомогою різних технологій, які розрізняються за дальністю, швидкістю, надійністю та стійкістю до перешкод. На рівні програмної архітектури ІКК охоплює модулі керування обміном даних, системи логічного контролю, механізми синхронізації процесів та засоби забезпечення безпеки. Програмне забезпечення відповідає за інтерпретацію сенсорних потоків, обробку телеметрії, аналіз внутрішнього стану платформи та узгодження дій різних частин комплексу. Важливою його функцією є реалізація протоколів обміну інформацією, завдяки яким забезпечується узгодженість дій сенсорів, виконавчих пристроїв і комунікаційних модулів. Виконавча підсистема забезпечує реалізацію команд, що генеруються на основі аналізу даних. До неї належать двигуни, приводи, сервомеханізми та інші елементи, які відповідають за переміщення платформи, виконання маніпуляцій або взаємодію з об'єктами в середовищі. Ефективність роботи виконавчої підсистеми значною мірою залежить від якості інформації, яку вона отримує від обчислювального ядра. Тому взаємодія між цими підсистемами має бути максимально узгодженою, а канали керування достатньо надійними для запобігання помилкам у критичних ситуаціях. Складною та водночас ключовою частиною структури ІКК є підсистема безпеки та контролю цілісності даних, яка відповідає за виявлення загроз, запобігання спробам втручання, контроль достовірності сенсорних потоків та захист каналів зв'язку від зовнішніх впливів. Структура ІКК має також включати засоби контролю технічного стану, які забезпечують постійне відстеження працездатності апаратних і програмних компонентів. Такі засоби дозволяють аналізувати телеметрію, оцінювати параметри енергоживлення, виявляти деградацію сенсорів та прогнозувати потенційні відмови. Механізми самодіагностики і самовідновлення забезпечують здатність платформи підтримувати стабільний режим функціонування без втручання оператора, що є критично важливим у складних або віддалених середовищах.

Узгоджена взаємодія всіх зазначених підсистем формує цілісну архітектурну модель ІКК, яка забезпечує повноцінний цикл обробки інформації – від сприйняття до виконання керуючих дій, від виявлення відхилень до прийняття рішень щодо усунення загроз або переходу до резервного режиму. Цілісність структури визначає здатність платформи ефективно функціонувати в умовах невизначеності, підвищених навантажень, інформаційного впливу або часткових технічних відмов. Таким чином, ІКК НМРП розглядається як ключовий елемент, що забезпечує автономність, надійність, живучість і стійкість роботизованої системи в цілому.

Рис. 1. Структура інформаційно-комунікаційного комплексу НМРП

Комплексний контроль дозволяє виявляти приховані або повільні деградації системи. До критичних параметрів ІКК належать:

1. Стан сенсорних модулів (рівень сигналу; достовірність і частота вимірювань; кореляція між даними різних сенсорів; наявність аномальних станів, шумів, затримок).

2. Стан каналів зв'язку (рівень інтенсивності прийнятого сигналу (RSSI); пропускна здатність; затримки передачі; втрати пакетів; спроби несанкціонованого доступу).

3. Стан обчислювального комплексу (завантаженість процесора; температурні режими; відмови модулів; затримки обробки телеметрії).

4. Стан виконавчих модулів (стабільність роботи приводів; відгук системи керування на вхідні сигнали; коректність виконання команд).

Архітектура системи моніторингу ІКК НМРП є багаторівневою, яка функціонує поверх апаратних та

програмних підсистем НМРП. На відміну від базових модулів платформи, система моніторингу має власну логічну структуру, орієнтовану не на виконання місії чи управління рухом, а на безперервне спостереження за технічним станом, параметрами середовища та станом інформаційно-комунікаційних каналів. Мета – підтримання моніторингового контролю щодо внутрішніх і зовнішніх процесів, прогнозування потенційних відмов та забезпечення стійкості платформи у змінних середовищах.

Основою архітектури є модуль збору діагностичних даних, який приймає телеметрію від сенсорів, виконавчих пристроїв, процесорних модулів та мережевих інтерфейсів, і забезпечує первинний прийом інформаційних потоків з різною частотою оновлення та різною структурою. У межах цього компонента здійснюється синхронізація часових міток, фільтрація шумів, нормалізація параметрів і перетворення їх у єдиний уніфікований формат, придатний для подальшої обробки. Наступним функціональним блоком архітектури є модуль аналітичної обробки та фільтрації, завдання якого полягає у виявленні закономірностей у потокових даних, контролю показників у допустимих межах та визначенні можливих відхилень у роботі підсистем. У модулі використовуються статистичні методи, фільтри реального часу та інтелектуальні механізми попередньої діагностики. Важливою складовою архітектури є модуль виявлення аномальних станів, який виконує функцію глибокого аналізу відхилень у поведінці параметрів. На цьому рівні система розпізнає комплексні нестандартні патерни у часових рядах, що можуть свідчити про ранні стадії технічної непрацездатності, зовнішнє втручання або деградацію апаратного компонента. Алгоритми модуля ґрунтуються на концепціях машинного навчання, кластеризації, побудові поведінкових моделей та взаємних кореляційних зв'язків між параметрами. Аномалії класифікуються за ступенем критичності, що дозволяє системі реагувати диференційовано. Вищим рівнем функціонування є модуль прогнозування, який виконує прогнозне моделювання технічного стану платформи. Прогнозні алгоритми дозволяють оцінювати залишковий ресурс силової установки, акумуляторів, сенсорних модулів та обчислювальних систем. Модуль формує сценарії розвитку подій, які допомагають системі завчасно переходити в резервні режими, обмежувати навантаження на окремі вузли або змінювати параметри роботи ІКК для запобігання стану непрацездатності системи. Суттєвою частиною архітектури є модуль візуалізації стану, який забезпечує подання діагностичних даних для оператора або зовнішньої системи контролю. У модулі здійснюється побудова графічних індикаторів, теплових карт, діаграм залежностей та інших форм інтерфейсів, що дозволяють оцінювати технічний стан платформи у реальному часі.

Загальна логіка роботи архітектури системи моніторингу передбачає проходження даних через послідовність етапів: телеметрія надходить від сенсорів та підсистем управління, проходить первинну обробку і фільтрацію, аналізується на предмет відповідності нормам і можливих відхилень, після чого переходить до рівня інтелектуального аналізу та прогнозування, а далі – до системи інформування, яка формує реакцію та сигналізує про необхідність дій з боку керуючих модулів або оператора. Така послідовність дозволяє забезпечити повний цикл контролю стану платформи.

Багаторівнева архітектура системи моніторингу включає базовий рівень технічного моніторингу, де відстежуються основні параметри роботи апаратних компонентів; рівень функціональної діагностики, що забезпечує аналіз стану окремих підсистем; рівень інтелектуального аналізу, який відповідає за виявлення складних аномальних станів та рівень стратегічного прогнозування, що визначає поведінку системи у перспективі. Кожен з цих рівнів реалізує окрему групу алгоритмів і взаємодіє з іншими через внутрішню логічну шину (рис. 2).

Рис. 2. Архітектура системи моніторингу інформаційно-комунікаційного комплексу НМРП

Інформаційна безпека ІКК НМРП є однією з ключових умов забезпечення стабільної роботи платформи та збереження цілісності всіх процесів управління. Оскільки НМРП функціонують у середовищах з неоднорідними умовами, у тому числі з потенційною присутністю зовнішніх зловмисних впливів, система

безпеки повинна забезпечувати надійний захист каналів зв'язку, внутрішніх інформаційних потоків і сенсорних даних. Система інтегрується у загальну архітектуру моніторингу та взаємодіє з діагностичними модулями, що дає змогу виявляти не тільки технічні відмови, а й інформаційні загрози різного типу. Основою захисту телекомунікаційних каналів є застосування сучасних криптографічних механізмів, які забезпечують конфіденційність, цілісність та автентичність переданої інформації. Шифрування каналів із використанням алгоритмів типу AES та RSA дозволяє унеможливити перехоплення або модифікацію даних у процесі передачі. Симетричні алгоритми забезпечують високу швидкість шифрування телеметрії, тоді як асиметричні алгоритми використовуються для захисту команд управління, забезпечуючи гарантовану перевірку джерела даних. Завдяки цьому команда, що надходить до платформи, може бути оброблена лише після підтвердження її автентичності. Система аналізу трафіку є наступним важливим компонентом інформаційної безпеки, яка здійснює контроль усіх мережевих потоків, аналізує частоту, структуру, обсяг та часові характеристики переданої інформації. При виявлення аномальних станів, таких як різке збільшення навантаження на канал, несумірність обсягу даних зі звичайною діагностичною активністю або нетипові патерни пакетів, система сигналізує про потенційну атаку. Одним із критичних аспектів забезпечення інформаційної безпеки є виявлення спуфінгу навігаційних сигналів. НМРП використовують навігаційні системи для визначення свого положення у просторі, тому заміна або спотворення навігаційних даних може спричинити втрату керованості. Для запобігання цьому застосовуються алгоритми контролю узгодженості між кількома незалежними джерелами навігаційної інформації.

Результатом вищенаведеної архітектури є формування багаторівневої системи захисту, яка забезпечує не лише реагування на вже виявлені загрози, а й запобігає їх появі шляхом постійного моніторингу, аналізу та прогнозування. Інформаційна безпека ІКК розглядається не як окремий модуль, а як інтегрована складова, що пронизує всі рівні управління та функціонування платформи. Комплексний характер такої системи дозволяє забезпечити високу стійкість до зовнішніх впливів і гарантувати цілісність, достовірність і доступність даних, необхідних для безпечної роботи НМРП.

На рис. 3 наведено приклад інтерфейсу системи моніторингу ІКК НМРП.

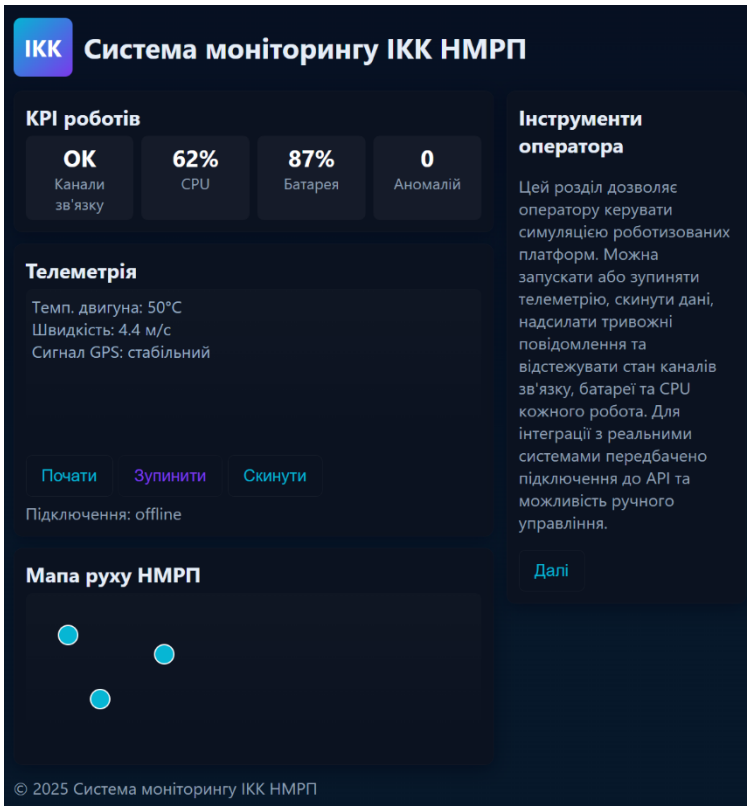

Рис. 3. Приклад інтерфейсу системи моніторингу ІКК НМРП

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У роботі сформовано комплексну концепцію системи моніторингу інформаційно-комунікаційного комплексу наземних мобільних роботизованих платформ, що інтегрує структурний аналіз комплексу, визначення ключових параметрів контролю, розробку багаторівневої архітектури моніторингу та механізмів інформаційної безпеки. Проведений аналіз сучасних підходів підтвердив, що ефективна робота наземних мобільних роботизованих платформ значною мірою залежить від наявності постійного контролю технічних, функціональних і комунікаційних процесів, а також від ступеню захищеності каналів передачі даних.

Розроблена архітектура системи моніторингу передбачає послідовну роботу модулів збору даних, аналітичної обробки, виявлення аномальних станів та прогнозування, що забезпечує швидке реагування на

відхилення у роботі підсистем, дозволяє виявляти як внутрішні технічні відмови, так і відхилення, спричинені зовнішніми впливами. Інтегровані механізми інформаційної безпеки, включаючи криптографічний захист, аутентифікацію команд, аналіз трафіку та виявлення навігаційного спуфінгу, створюють додатковий рівень стійкості платформи до кіберзагроз.

Комплексність підходу забезпечує можливість адаптації архітектури під різні типи роботизованих платформ і відкриває перспективи подальших досліджень у напрямі цифрових двійників, розширених моделей прогнозування та автономних систем безпеки, а також побудови розподіленої обчислювальної інфраструктури, яка забезпечить обробку телеметрії у режимі реального часу із мінімальною затримкою. Значний потенціал мають дослідження, спрямовані на розроблення масштабованої моніторингової архітектури, адаптованої до колективної взаємодії платформ у складних умовах.

Література

1. Correll N., Hayes B., Heckman C., Roncone A. Introduction to Autonomous Robots: Mechanisms, Sensors, Actuators, and Algorithms. 1st Edition. MIT Press, 2022. – 288 p.

2. Bozorgi H., Ngo T.D. Beyond Shared Autonomy: Joint Perception and Action for Human-In-The-Loop Mobile Robot Navigation Systems. Journal of Intelligent and Robotic Systems: Theory and Applications, 2023. – 109 (1), 20.

3. Billard A., Mirrazavi S., Figueroa N. Learning For Adaptive And Reactive Robot Control: A Dynamical Systems Approach / Massachusetts Institute of Technology. – MIT Press, 2022. – 424 p.

4. Ніконов О.Я., Філіпов В.В. Концепція багаторівневої інтелектуальної технології управління наземними мобільними роботизованими платформами // Вісник Хмельницького національного університету. Технічні науки. – 2025. – №5.2 (357). – С. 253–259.

5. Achouch M., Dimitrova M., Ziane K., Karganroudi S., Dhouib R., Ibrahim H., Adda M. On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges. Applied Sciences, – 2022. 12(16), 8081.

6. Fan Z., Zhang L., Wang X., Shen Y., Deng F. LiDAR, IMU, and camera fusion for simultaneous localization and mapping: a systematic review. Artificial Intelligence Review, 2025. – 58, 174. – P. 1–59.

7. Skvorchevsky A. Increasing the robustness of computer networks by using hybrid centralized-distributed topology, 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022. – P. 239–242.

8. Kumar M.S., Kasbekar G.S., Maity A. Identification of GPS Spoofing as a Drone Cyber-vulnerability and Evaluation of Efficacy of Asynchronous GPS spoofing. IFAC-PapersOnLine, 2022.– V.55, 22. – P. 394–399.

References

1. Correll N., Hayes B., Heckman C., Roncone A. Introduction to Autonomous Robots: Mechanisms, Sensors, Actuators, and Algorithms. 1st Edition. MIT Press, 2022. – 288 p.

2. Bozorgi H., Ngo T.D. Beyond Shared Autonomy: Joint Perception and Action for Human-In-The-Loop Mobile Robot Navigation Systems. Journal of Intelligent and Robotic Systems: Theory and Applications, 2023. – 109 (1), 20.

3. Billard A., Mirrazavi S., Figueroa N. Learning For Adaptive And Reactive Robot Control: A Dynamical Systems Approach / Massachusetts Institute of Technology. – MIT Press, 2022. – 424 p.

4. Nikonov O.Ya., Filipov V.V. Kontseptsiia bahatorivnevoi intelektualnoi tekhnolohii upravlinnia nazemnymy mobilnymy robotyzovanymy platformamy // Herald of Khmelnytskyi National University. Technical sciences. – 2025. – №5.2 (357). – S. 253–259.

5. Achouch M., Dimitrova M., Ziane K., Karganroudi S., Dhouib R., Ibrahim H., Adda M. On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges. Applied Sciences, – 2022. 12(16), 8081.

6. Fan Z., Zhang L., Wang X., Shen Y., Deng F. LiDAR, IMU, and camera fusion for simultaneous localization and mapping: a systematic review. Artificial Intelligence Review, 2025. – 58, 174. – P. 1–59.

7. Skvorchevsky A. Increasing the robustness of computer networks by using hybrid centralized-distributed topology, 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022. – P. 239–242.

8. Kumar M.S., Kasbekar G.S., Maity A. Identification of GPS Spoofing as a Drone Cyber-vulnerability and Evaluation of Efficacy of Asynchronous GPS spoofing. IFAC-PapersOnLine, 2022.– V.55, 22. – P. 394–399.